Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2013-05-23 (ITC-3463)
Certification No.	C0429
Sponsor	KONICA MINOLTA, INC.
TOE Name	bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e PKI Card System Control Software
TOE Version	A61F0Y0-0100-G00-09pki
PP Conformance	None
Assurance Package	EAL3
Developer	KONICA MINOLTA, INC.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Information Security Evaluation Office

This is to report that the evaluation result for the above TOE is certified as follows.
2014-04-28

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center
Technology Headquarters

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4 (Japanese Translation)
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4 (Japanese Translation)

Evaluation Result: Pass

"bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e PKI Card System Control Software" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e PKI Card System Control Software Version A61F0Y0-0100-G00-09pki" (hereinafter referred to as the "TOE") developed by KONICA MINOLTA, INC., and the evaluation of the TOE was finished on 2014-04 by Mizuho Information & Research Institute, Inc., Information Security Evaluation Office (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, KONICA MINOLTA, INC., and provide security information to procurement personnel and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is the appendix of this report together. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes "procurement personnel who purchase this TOE that is commercially available" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e, which this TOE is installed, are digital Multi Functional Peripheral (hereinafter all the products are referred to as "MFP."), provided by KONICA MINOLTA, INC., composed by selecting and combining each functions of copy, print, scan and FAX.

The TOE is the "bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e PKI Card System Control Software" that controls the entire operation of MFP, including the operation control processing and the image data management triggered by the panel of the main body of MFP or through the network. The TOE provides the protection function for the disclosure of the highly confidential documents stored in MFP. This TOE does not support the audit log function.

Moreover, against the danger of illegally bringing out HDD that is the medium to store image data in MFP, the TOE can prevent unauthorized access by encrypting image data written in HDD by using ASIC. Besides, the TOE provides the function that deletes data area including image data stored in HDD completely by deletion method compliant with various overwrite deletion standards and the function that controls the access from the FAX public line against the danger of using Fax function as a steppingstone to access internal network.

Regarding these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated in the range of the assurance package. Threats and assumptions that this TOE assumes are described in the next clause.

1.1.2.1 Threats and Security Objectives

This TOE counters each threat with the following security functions.

- It is assumed as threat that information leaks from MFP after lease-return or discard of MFP. To counter this threat, the TOE has the function to delete the information in storage medium.

- It is assumed as threat that HDD is stolen from MFP and information is leaked from stolen HDD. To counter this threat, the TOE encrypts and writes information in HDD by using the encryption function of ASIC, which is outside the scope of the TOE.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

It assumes that MFP including this TOE is installed in an office which is managed by an organisation such as a company or its section, and is connected to the intra-office LAN.

It assumes that IC card reader is usable with MFP and a client PC, and SMTP server is usable at LAN.

In this environment, MFP is managed not to be accessed from an external network when LAN is connected to an external network (outside of the organisation such as internet).

It assumes that an administrator and a service engineer are reliable. For example, it assumes that they can keep the secret about their password and an encryption passphrase.

It assumes that IC card, used in the use of the TOE, is limited to rightful user only.

It assumes that this TOE is used in the condition where the setting of enhanced security function is enabled.

1.1.3 Disclaimers

- Encryption of the communication of image files, a digital signature, the IC card using for authentication, IC card reader, exclusive driver, and the function of Active Directory are not assured in this evaluation.

- The encryption function by ASIC installed in MFP is not assured in this evaluation.

- The TOE supports the information deletion function of storage medium for the measure of leaking information when MFP is discarded or returned. However, it is not assured in this evaluation that the information of setting values such as passwords does not remain in the area of SSD, which is unable to be accessed from the TOE (this kind of area might exist by the characteristics of SSD.).

- Fax unit control function is valid only when the Fax unit as an optional part is installed.

- It is necessary to activate the setting of enhanced security function. When it is valid, a part of MFP functions cannot be used. Refer to the description of each settings written in "1.4.3.5 Enhanced Security Function" of the ST.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2014-04, based on functional requirements and assurance requirements of the TOE according to the publicised documents "IT Security Evaluation and Certification Scheme"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] prepared by the Evaluation Facility as well as evaluation evidential materials, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight review was also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e PKI Card System Control Software
TOE Version:	A61F0Y0-0100-G00-09pki
Developer:	KONICA MINOLTA, INC.

At the time of TOE installation, etc., a user can ask a service engineer as below to confirm that the product is the evaluated and certified TOE.

TOE version and checksum are displayed by panel operation of service engineer. A user can confirm that the installed product is the evaluated and certified TOE, by confirming TOE version and that checksum is same as one in a service manual.

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organisational security policies.

The TOE provides an encryption function with ASIC and an overwrite deletion function to prevent the leakage of information when MFP is returned or discarded, or HDD is taken illegally.

This TOE realizes the following functions for customer's demand.

- For highly confidential image files, a mechanism to encrypt when sending and receiving, to give a digital signature when sending from the TOE, and to print by only a user who sent when the TOE received.

- A mechanism not to permit access from an FAX public line port of MFP to an internal network

3.1 The Roles related to the TOE

The roles related to this TOE are defined as follows.

(1) User
An MFP user who owns IC card (In general, an employee in the office is assumed.)

(2) Administrator
An MFP user, who manages the operations of MFP, manages MFP's mechanical operations and users. (In general, it is assumed that the person elected among the employees in the office plays this role.)

(3) Service engineer
A user, who manages the maintenance for MFP, performs the repair and adjustment of MFP. In general, a person in charge of the maintenance service of MFP at a sales company in cooperation with KONICA MINOLTA, INC., is assumed.

(4) Responsible person of the organisation that uses MFP
A responsible person of the organisation that manages the office where MFP is installed. An administrator who manages the operation of MFP is assigned.

(5) Responsible person of the organisation that manages the maintenance of MFP
A responsible person of the organisation that manages the maintenance of MFP. A service engineer who manages the maintenance of MFP is assigned.

Besides these, though not a user of the TOE, those who go in and out the office are assumed to be accessible persons to the TOE.

3.2 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.2.1, and to satisfy the organisational security policies shown in Chapter 3.2.2.

3.2.1 Threats and Security Function Policies

3.2.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the security functions to counter them.

Table 3-1 Assumed Threats

Identifier	Threat
T.DISCARD-MFP (Lease-return and discard of MFP)	When leased MFPs are returned or when discarded MFPs are collected, encrypted print files, scanned image files, and stored image files can be leaked by a person with malicious intent when he/she analyzes the HDD in MFP.
T.BRING-OUT-STORAGE (Unauthorized bringing out HDD)	- Encrypted print files, scanned image files, and stored image files can be leaked by a person or a user with malicious intent, who illegally brings them out to analyze the HDD in MFP. - A person or a user with malicious intent illegally replaces HDD in MFP. In the replaced HDD, newly created files, such as encrypted print files, scanned image files, and stored image files are accumulated. A person or a user with malicious intent brings them out to analyze the replaced HDD, so such image files will be leaked.

3.2.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

(1) Security function to counter the threat [T.DISCARD-MFP (Lease-return and discard of MFP)]

This threat assumes the possibility of leaking information from MFP collected from users.

The TOE provides the function to overwrite data for the deletion of data area including image data in HDD, so it prevents the leakage of the protected assets stored in HDD connected to lease-returned MFPs or discarded MFPs.

The following methods can be chosen as the overwrite deletion method. (For example, it indicates that the first one overwrites once by 0x00 and that the second one overwrites in the order of Random numbers, Random numbers, and 0x00. "Verification" means to check that the last overwriting was executed correctly by actually reading the HDD.)

- 0x00
- Random numbers => Random numbers => 0x00
- 0x00 => 0xFF => Random numbers => Verification
- Random numbers => 0x00 => 0xFF

- 0x00 => 0xFF => 0x00 => 0xFF
- 0x00 => 0xFF => 0x00 => 0xFF => 0x00 => 0xFF => Random numbers
- 0x00 => 0xFF => 0x00 => 0xFF => 0x00 => 0xFF => 0xAA
- 0x00 => 0xFF => 0x00 => 0xFF => 0x00 => 0xFF => 0xAA => Verification

(2) Security function to counter the threat [T.BRING-OUT-STORAGE (Unauthorized bringing-out of HDD)]

This threat assumes the possibility that the image data in HDD to be leaked by being stolen from the operational environment where MFP is used, or by installing the unauthorized HDD and bringing it out with the image data accumulated in it.

By using the encryption function of ASIC, which is outside the scope of the TOE, this TOE provides the generation function of encryption key to encrypt the data written in the HDD (referred to as "encryption key generation function") and supporting function with the ASIC (referred to as "ASIC operation support function"), so that the encrypted image data are stored in HDD, and it makes it difficult to decode the data even if the information is read out from HDD.

3.2.2 Organisational Security Policies and Security Function Policies

3.2.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE are shown in Table 3-2.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.COMMUNICATION-CRYPTO (Encryption communication of image files)	Highly confidential image files (encrypted print files, scanned image files) which transmitted or received between IT equipments must be encrypted.
P.COMMUNICATION-SIGN (Signature of image files)	A digital signature must be added to a mail including highly confidential image files (scanned image files).
P.DECRYPT-PRINT (Decryption of image files)	Highly confidential image files (encrypted print files) received by MFP are permitted to print only to a user who generated those files.
P.REJECT-LINE (Access prohibition from public line)	An access to internal network from public line via the Fax public line portal must be prohibited.

The term "between IT equipments" here indicates between client PC and MFP that a user uses.

3.2.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the security functions to satisfy the organisational security policies shown in Table 3-2.

(1) Security function to satisfy the organisational security policy [P.COMMUNICATION-CRYPTO (Encryption communication of image files)]

This organisational security policy regulates that image files which flows on network are encrypted to ensure the confidentiality. As this corresponds according to one's request, it does not need to encrypt all image data. It needs to encrypt data between MFP and user's client PC in handling encrypted print files or scan image files.

In this TOE, by supporting the function to encrypt scanned image files sent by e-mail from MFP to user's own client PC (referred to as "S/MIME encryption function") and by encrypting the encrypted print files sent from the client PC to MFP using the exclusive driver and an IC card, which is outside the scope of this TOE, it is possible to securely send and receive image files over the network.

(2) Security function to satisfy the organisational security policy [P.COMMUNICATION-SIGN (Signature of image files)]

This organisational security policy regulates that a signature is added to image files to be sent or received by e-mail in order to secure the integrity of the files. Because this function only needs to be available upon request, a signature does not need to be appended to all image files, except that any scanned image files to be handled need to have a signature.

The TOE has a function of interlocking with an IC card, which is outside the scope of the TOE, for scanned image files to be sent by e-mail from MFP to user's own client PC (referred to as "IC card operation support function") and a function of appending a signature to those scanned image files on its own (referred to as "S/MIME signature function"). With these functions, the TOE allows image files to be sent by e-mail while maintaining the integrity of the files.

(3) Security function to satisfy the organisational security policy [P.DECRYPT-PRINT (Decryption of image files)]

This organisational security policy regulates that only a user who generated an encrypted print file can decrypt and print that encrypted print file.

The TOE has a function of interlocking with an IC card, which is outside the scope of the TOE, for encrypted print files (referred to as "IC card operation support function") and a function that those encrypted print files can be accepted to decrypt and print when IC card which generated the encrypted print files is used (referred to as "encrypted print file decryption function"), only a user who generated the encrypted print files can decrypt and print the encrypted print files.

(4) Security function to satisfy the organisational security policy [P.REJECT-LINE (Access prohibition from public line)]

This organisational security policy prohibits being accessed to internal network via the port of Fax public line on Fax unit installed to MFP. This function is provided when Fax unit is installed to MFP.

This TOE provides the function which prohibits the access to the data existing in internal network from public line via the port of Fax public line (referred to as "Fax unit control function"), so that it enables to prohibit the access to the internal network via the port of Fax public line.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN (Personnel conditions to be an administrator)	Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.
A.SERVICE (Personnel conditions to be a service engineer)	Service engineers, in the role given to them, will not carry out a malicious act during series of permitted operations given to them.
A.NETWORK (Network connection conditions for MFP)	When the intra-office LAN where MFP with the TOE will be installed is connected to an external network, access from the external network to MFP is not allowed.
A.SECRET (Operational condition on secret information)	Each password and encryption passphrase shall not be leaked from each user in the use of the TOE.
A.IC-CARD (Operational condition on IC card)	IC card is owned by rightful user in the use of the TOE.

4.2 Environmental Assumptions

This TOE is installed in either bizhub 554e, bizhub 454e, bizhub 364e, bizhub 284e, or bizhub 224e, which is MFP provided by KONICA MINOLTA, INC. It assumes that IC card reader is connected to MFP. It is optional whether Fax unit is installed.

It assumes that MFP including this TOE is installed in an office which is managed by an organisation such as a company or its section, and is connected to the intra-office LAN.

It assumes that Active Directory is connected to the intra-office LAN to authenticate user's IC card.

It assumes that a client PC, which installed an exclusive printer driver and connected to IC card reader, is connected to the intra-office LAN.

It assumes that SMTP server is connected to the intra-office LAN. It is optional whether DNS server is used in the intra-office LAN.

It should be noted that the reliability of the hardware and the cooperating software shown in this configuration is out of the scope in the evaluation. Those are assumed to be trustworthy.

4.3 Clarification of Scope

The reliability of ASIC, IC card, IC card reader, exclusive driver, Active Directory, and SSD, in the following cases is not the scope of this evaluation.

- The TOE has the function to encrypt and write information in HDD, but the operation of the encryption is a function done by ASIC which is a part of MFP, so that it is outside the scope of the TOE and is not the scope of this evaluation.

- To realize the organisational security policies, an encryption of communicating image files, a digital signature and authentication are necessary. Though this TOE cooperates with IC card, IC card reader, exclusive driver and Active Directory, these are outside the scope of the TOE and are not the scope of this evaluation.

- There is a possibility that information on setting values such as passwords might remain in the area of SSD, which is unable to be accessed from the TOE (this kind of area might exist by the characteristics of SSD.). Such remaining information is protected by the difficulty of obtaining the remaining information from SSD. SSD is outside the scope of the TOE and the difficulty of obtaining the remaining information is not the scope of this evaluation.

5. Architectural Information

This chapter explains the scope and the main components (subsystems) of the TOE.

5.1 TOE Boundary and Components

The TOE is the software that controls the entire operation of MFP. It is installed in the SSD on MFP controller in the main body of MFP. It is loaded and run on the RAM when main power is switched ON. The relation between the TOE and MFP is shown in Figure 5-1.

In Figure 5-1, FAX unit marked as * is an optional part of MFP. It assumes that FAX unit is installed when a user uses FAX function.

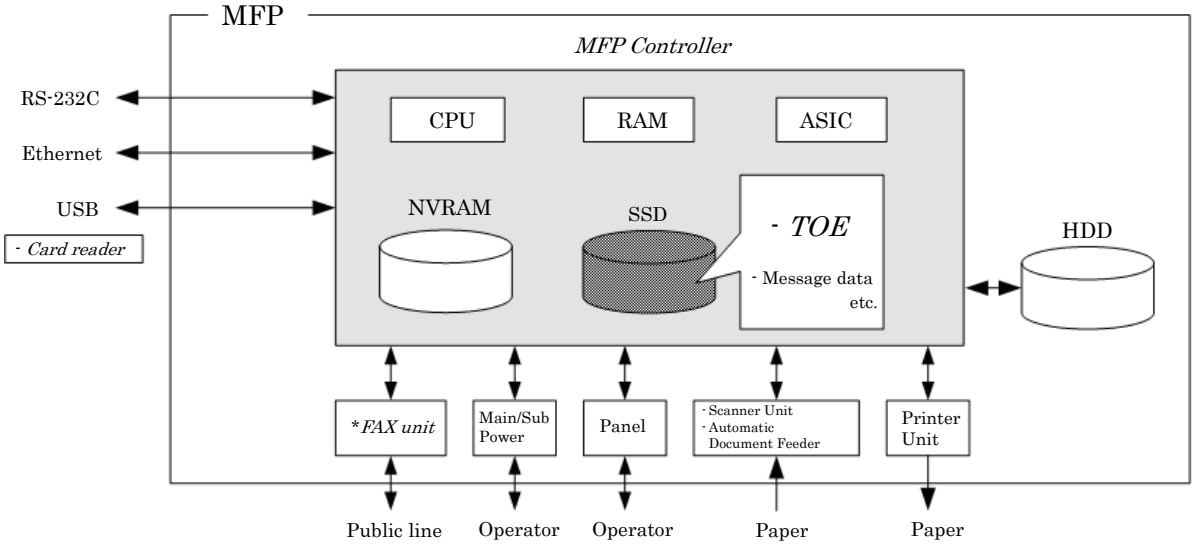

Figure 5.1 TOE boundary

The TOE is composed of an OS part and an application part which controls MFP. The application part which controls MFP is composed of the following parts further.

- The part which provides interface through the network
  It controls Ethernet and provides TCP/IP-based communication function.

- The part which provides interface via the panel
  It has the function which receives the input from the panel as well as the function which draws the screen of the panel.

- The part which performs job management
  A job means a unit for managing an execution control and operation order of copy, print, scan, Fax, user box file operation, and so on.
  The job is made and registered, when "the part which controls each device" receives the operation from "the part which provides interface through the network" or "the part which provides interface via the panel" and the reception from the Fax unit.
  The execution of the actual job is realized using the following parts, namely, "the part which executes common management," "the part which handles HDD," and "the part which controls each device."

- The part which executes common management
  This part manages various setting values and provides a measure for another part of the TOE to access to the setting value. Various setting values include information used to execute security functions, like authentication information.
  This part provides the function executing identification and authentication as well as the function of access control.
  This part realizes the following functions by using a function of IC card through IC card reader.
  > Encryption, decryption, and signature of S/MIME
  > Decryption of encryption print files

- The part which handles HDD
  This part provides the handling of image data and input/output function to HDD.
  In the input/output function of image data to HDD, an encryption at the time of writing and a decryption at the time of reading are done by ASIC.
  It overwrites all data of HDD with the directed method when an administrator indicates.

- The part which controls each device
  This part controls scanner unit, printer unit, and Fax unit, and realizes the actual work of Copy, Print, Scan and Fax.
  Moreover, it is the mechanism that does not allow access to an internal network from Fax unit.

- The part which provides support function
  This part provides functions used for support of MFP (function for diagnostics of MFP and function of updating the TOE).

5.2 IT Environment

The configuration of IT environment of this TOE in Figure 5-1 is explained as follows.

(1) SSD
A storage medium that stores the object code of the "MFP PKI Card System Control Software," which is the TOE. Additionally, it stores information on the setting values, such as passwords, and the message data expressed in each country's language to display the response to access through the panel and the network.

(2) NVRAM
A non-volatile memory. This memory medium stores various settings that MFP needs for the processing of the TOE. These setting values are managed in "the part which executes common management."

(3) ASIC
An integrated circuit for specific applications which implements HDD encryption functions for encrypting image data written in HDD. ASIC is used from "the part which handles HDD."

(4) HDD
A hard disk drive of 250GB in capacity. This is used not only for storing image data as files but also as an area to save image data temporarily during extension conversion, and so on. The loadable drivers for accessing an IC card are also stored here. It is read and written from "the part which handles HDD."

(5) Main/sub power supply
Power switches for activating MFP.

(6) Panel
An exclusive control device for the operation of MFP, equipped with a touch panel of a liquid crystal monitor, numeric keypad, start key, stop key, screen switch key, etc. It is controlled by "the part which provides interface via the panel."

(7) Scanner unit / automatic document feeder
A device that scans images and photos from paper and converts them into digital data. It is controlled by "the part which controls each device."

(8) Printer unit
A device that actually prints the image data which were converted for printing when receiving a print request by MFP controller. It is controlled by "the part which controls each device."

(9) Ethernet
It supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet. It is controlled by "the part which provides interface through the network."

(10) USB
It can be connected with a card reader corresponded to IC card. A card reader is not pre-installed in MFP as a standard for selling circumstances, but sold as an optional part. It is an essential component under this ST assumption.

(11) IC card
An IC card that supports the standard specification of Common Access Card (CAC) and Personal ID Verification (PIV).
It supports "the part which executes common management" by the function which decrypts a common key, operates a signature to message digest, and prepares a public key.

(12) RS-232C
Serial connection using D-sub 9 pins connectors is usable. The maintenance function is usable through this interface in case of failure.

(13) FAX Unit (*Optional part)
A device that has a port of Fax public line, which is used for transmitting and receiving FAX via the public line.
It is not pre-installed in the MFP as a standard for selling circumstances, but sold as an optional part. Fax unit is purchased when an organisation needs it, and the installation is not indispensable.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

< For administrators and users >

- bizhub 554e / 454e / 364e / 284e / 224e for PKI Card System User's Guide [Security Operations] Ver.1.01

< For service engineers >

- bizhub 554e / 454e / 364e / 284e / 224e for PKI Card System SERVICE MANUAL SECURITY FUNCTION Ver.1.01

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.2 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2013-05 and concluded upon completion of the Evaluation Technical Report dated 2014-04. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Additionally, for site inspections, considering the previous inspections for the same series of the TOE, the evaluator directly visited the development and manufacturing sites on 2013-07, 2013-10 and 2013-12 and examined procedural status of configuration management, delivery, and security measures, focusing on the different parts of those from the same series of the TOE, by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2013-12.

Concerns that the Certification Body found in the evaluation process were described as the certification oversight review, and it was sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

7.3 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As a result of the evidence shown in the process of the evaluation and those confirmed validity, the evaluator performed the reproducibility testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of actual testing results. The content of the developer testing evaluated by the evaluator is explained as follows.

1) Developer Testing Environment

Figure 7-1 shows the testing configuration performed by the developer.

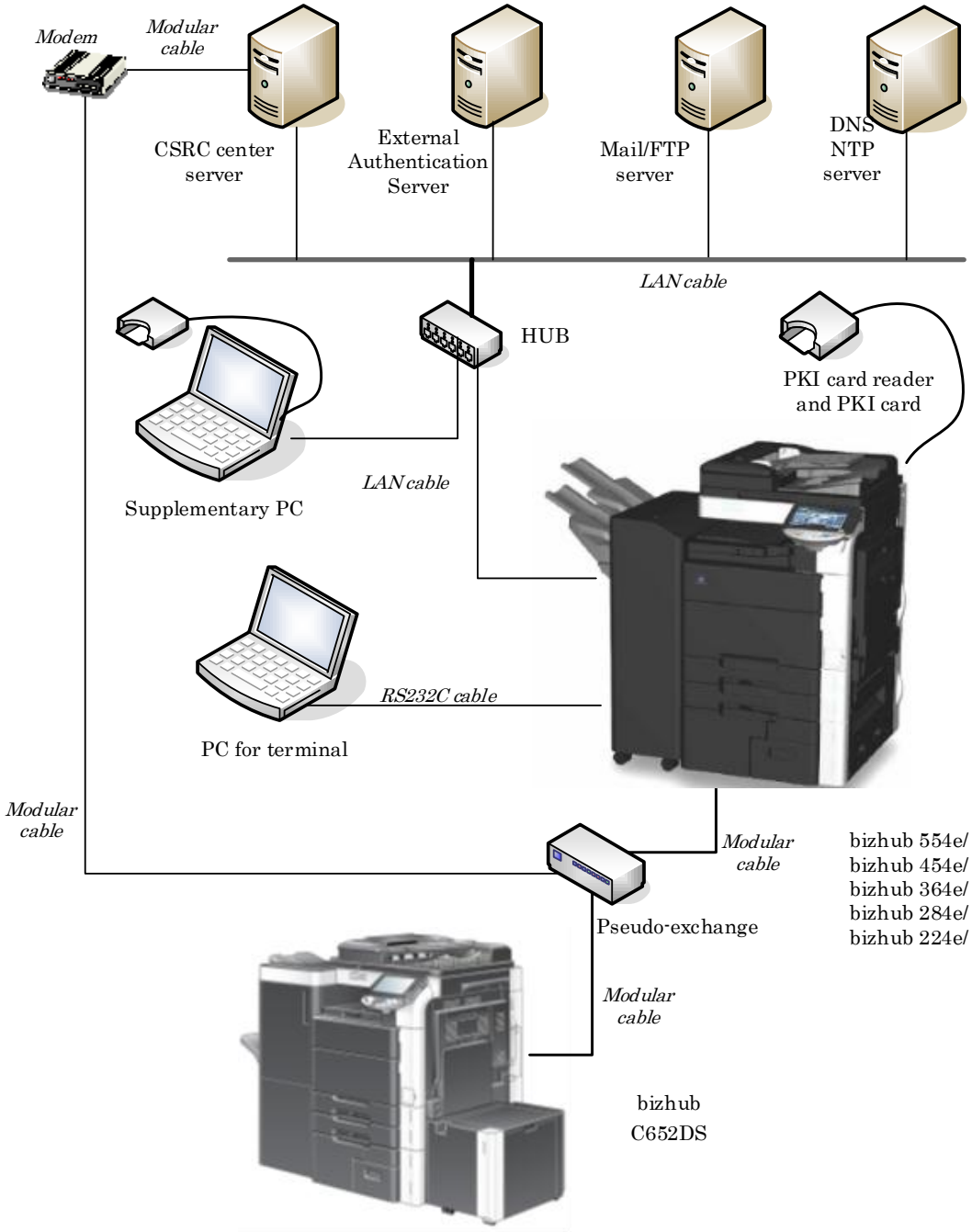

Figure 7-1 Configuration of the Developer Testing

The developer testing was performed in the same TOE testing environment as the TOE configuration identified in the ST.

2) Summary of the Developer Testing

A summary of the developer testing is as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

The testing was conducted to execute security functions through the external interface when the functions which have the external interfaces that the developer can use. It was conducted to obtain and analyze the executed results of security functions through dump tool or capturing tool of communication data when functions do not have the external interfaces that the developer can use.

<Developer Testing Tools>

Table 7-1 shows tools used in the developer testing.

Table 7-1 Developer Testing Tools

Name of Device and Software	Outline and Purpose of Use
KONICA MINOLTA 554e Series PCL Driver Ver. 1.1.3.OSW1_01	Exclusive printer driver software for bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e PKI Card System. It is used for encrypted print.
ActiveClient 6.1	Driver software for smart card. It is used as a driver for PKI card in the supplementary PC.
SCR3310 USB Smart Card Reader Driver V4.41	Driver software for PKI card reader. It is used after installing to the supplementary PC.
WireShark Ver. 1.2.2	Software tool for monitoring and analyzing the communication on the LAN. It is used for getting communication log and confirming data.
Mozilla Thunderbird Ver. 2.0.0.21	General purpose mailer software. It is used as a confirmation tool of S/MIME mail on the supplementary PC.
Open SSL Ver. 1.0.0d (8-Feb-2011)	Software tool for hash function and encryption/decryption function. It is used for confirming S/MIME signature.
Tera Term Pro Ver. 4.29	Terminal software executed in the terminal PC. It is used to connect with MFP and to operate the terminal software installed in MFP to monitor the state of the TOE.
Disk dump editor Ver. 1.4.3	Software tool to display the contents in HDD. It is used for confirming the contents of HDD.
Stirling Ver. 1.31	Binary editor software tool. It is used for confirming the contents of decode S/MIME messages.
MIME Base64 Encode/Decode v1.0	Software tool for encoding/decoding of MIME Base64. It is used for decoding S/MIME messages.
Blank Jumbo Dog Ver. 4.2.2	Simple server software for intranet. It is used as mailer server and FTP server function.
CSRC center software Ver. 2.7.0	Server software for CSRC center. CSRC is a maintenance service, which KONICA MINOLTA, INC., offers, to manage the state of MFP by remote.

b. Scope of the Performed Developer Testing

The developer testing was performed on 53 items by the developer. By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested. By the depth analysis, it was verified that all the subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

c. Result

The evaluator confirmed the approach of the performed developer testing and the legitimacy of tested items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach. The evaluator confirmed consistencies between the testing results expected by the developer and the actual testing results performed by the developer.

7.3.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of security functions by the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to ensure that security functions are certainly implemented from the evidence shown in the process of the evaluation.
The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The configuration of the testing performed by the evaluator is the same configuration with the developer testing. KONICA MINOLTA 554e Series PCL Driver and CSRC center software that were used for the developer testing were used, but these specification confirmation, operation tests, and calibration were executed by the evaluator.

As the result of the following confirmation by the evaluator, there is no problem with selecting only bizhub 554e / bizhub 364e as the MFP which the TOE is installed.

- The evaluator confirmed that the difference between bizhub 545e, bizhub 454e, bizhub 364e, bizhub 284e and bizhub 224e is the copy/print speed, durability guaranteed value and the configuration of paper feeding and ejection, by the provided documents from the developer. It was judged that these differences do not affect the behavior of the tests that were performed by the evaluator.

2) Summary of the Independent Testing

A summary of the independent testing is as follows.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluator designed from the developer testing and the provided evaluation evidential materials are shown below.

<Viewpoints of Testing >

(1) Based on the situation of the developer testing, test as many security functions as possible.
(2) Test all probabilistic and permutable mechanism.

(3) Test behaviors depending on the differences of password input methods to TSFI for the testing of the probabilistic and permutable mechanism.
(4) Test the variations supplementing the developer testing on illegal input value.
(5) Based on the complexity of interfaces, test the necessary variations.
(6) For the interfaces with innovative and unusual characters, test the necessary variations.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

The testing was conducted to execute security functions through the external interface when the functions have the interfaces that the evaluator can use. It was conducted to obtain and analyze the executed results of security functions through dump tool or capturing tool of the transmitted data when the functions do not have the external interfaces that the evaluator can use.

<Independent Testing Tools>

The tools, etc., used at the testing are the same as those used at the developer testing.

<Content of the Performed Independent Testing>

An outline of each independent testing viewpoint is shown in Table 7-2.

Table 7-2 Viewpoints of Independent Testing and Overview of Testing

Viewpoints of Independent Testing	Overview of Testing
(1) Viewpoint	Testing was performed, which was judged to be necessary in addition to the developer testing.
(2) Viewpoint	Testing was performed with changing the digit number of characters and the types of characters by paying attention to the probabilistic and permutable mechanism at the identification and authentication, etc., by the administrator.
(3) Viewpoint	Testing was performed with consideration for the operated interfaces to confirm behaviors depending on the difference of password input methods.
(4) Viewpoint	Tests that are different variation from the developer testing were performed on the exception value of the minimum number of characters for passwords.
(5) Viewpoint	Testing was performed with consideration for the complexity of S/MIME encryption function to confirm actions when encrypting scanned image data and transmitting by e-mail.
(6) Viewpoint	Testing was performed to confirm actions by judging the functions, such as Fax unit control function, encryption key generation function of HDD encryption, and encryption print function, to be innovative or not general.

c. Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.3.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation. The penetration testing performed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided evidence and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

<Vulnerability requiring the penetration testing>

(1) There is a possibility that the unexpected services related to the components used for the TOE might be activated.
(2) There is concern about the existence of the vulnerabilities within the public domain related to the components used for the TOE.
(3) When retrieving the developer evidential materials, it was detected that there is concern that security functions might be bypassed or falsified, depending on the timing of the power ON/OFF.
(4) When retrieving the developer evidential materials if there is concern about attacks by wiretapping communications, it could not reach certainty that there is no concern of attacks to the communications between card reader and MFP or between the related MFP and the external authentication server.
(5) As it is known from the ST, several types of interfaces supporting the authentication function exist. From the development evidential materials, considering cases when authentication from different types of interfaces competes with each other, it is concerned that there is a possibility of being operated by an operator with different authority.
(6) As it is known from the developer evidential materials, several mechanisms protect the data in HDD from being read, even when HDD is brought out and connected to the same types of MFP. However, it is uncertain about a part of operation of mechanism.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

Figure 7-2 shows the penetration test configuration used by the evaluator.

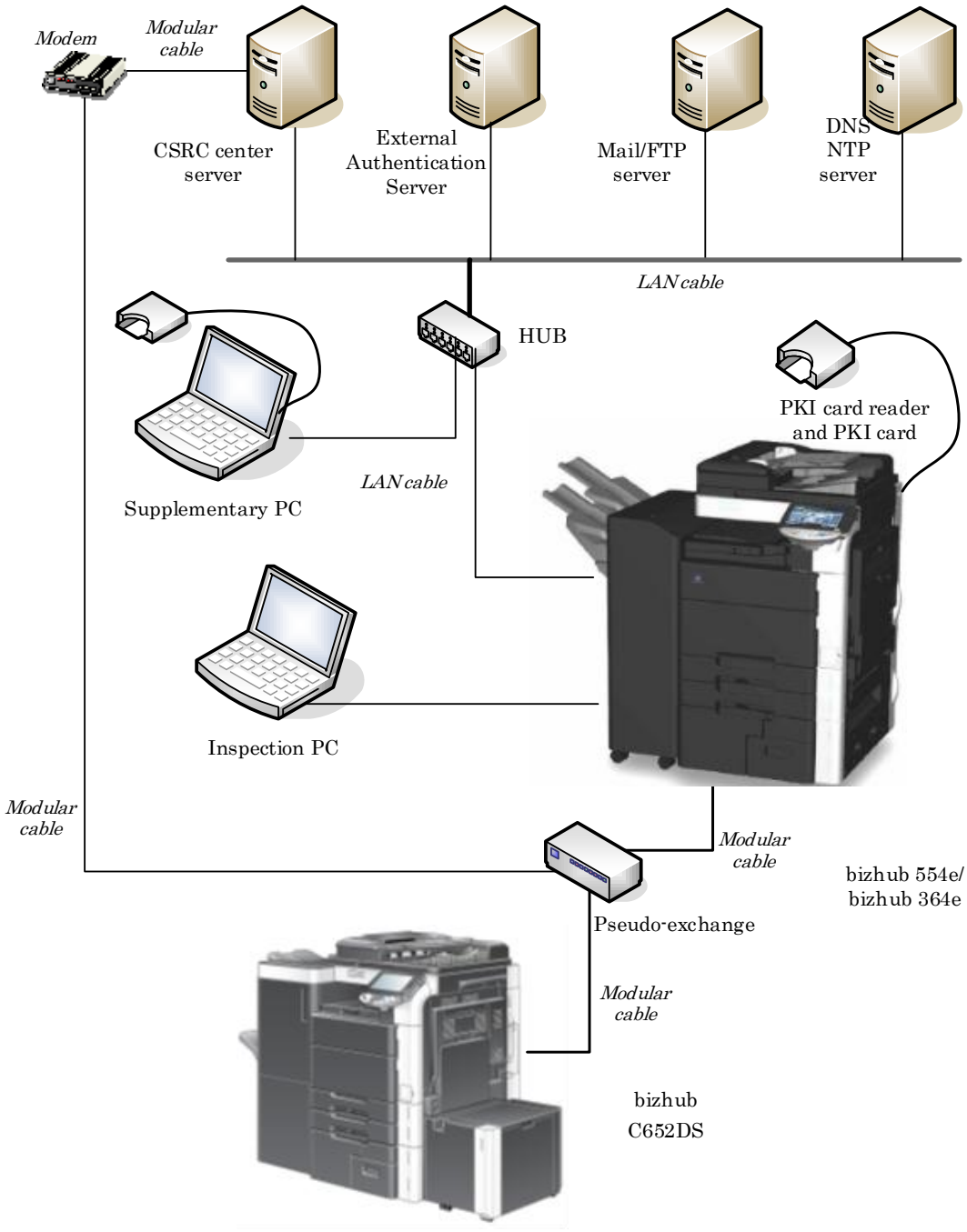

Figure 7-2 Penetration Testing Environment

<Penetration Testing Approach>

The testing was conducted using the following methods; a method to check with the visual observation of the behavior after stimulating the TOE by operating from the operational panel, a method to check with the visual observation of the behavior after accessing the TOE through network with operating the supplementary PC, a method to check the behavior with test tools by using test tools, a method to check authentication operation by using IC card, a method to check data transferred between IC card and the TOE in authentication process, and a method to scan the publicly-known vulnerabilities with the vulnerability checking tool by operating the inspection PC.

<Tools and others used at Penetration Testing>

The tools, etc., used at the penetration testing are shown in Table 7-3.

Table 7-3 Configuration of Penetration Testing

Testing Configuration Environment	Details
Inspection object (TOE)	- The TOE installed in bizhub 554e / bizhub 364e (Version: A61F0Y0-0100-G00-09pki) - Network configuration The penetration testing was done by connecting each MFP with hub or cross-cable.
Supplementary PC	- PC with network terminal operated on Windows XP SP3. - The tools shown in Table 7-1 (Thunderbird, Disk dump editor, etc.) and software for USB analyzer (made by Catalyst Enterprises) were also used. - By connecting to MFP by using printer driver, IC card, etc., it is possible to use the encryption print function.
Inspection PC	- Inspection PC is a PC with network terminal operated on Windows XP SP3, and is connected to MFP with cross-cable to perform vulnerability testing. - Explanation of testing tools (The operational checks of the following tools are finished under network environment in Mizuho Information & Research Institute, Inc. The latest versions of plug-in and vulnerability database as of December 3, 2013, are applied.) (1)snmpwalk Version 3.6.1 MIB information acquiring tool (2)openSSL Version 0.9.8y Encryption tool of SSL and hash function (3)Nessus 5.2.4 Security scanner to inspect vulnerabilities existing on the system (4)WireShark 1.10.3 Packet analyzer software that can analyze more than 800 protocols (5)extrstr 0.2 Binary analyzer tool that the Evaluation Facility developed. By using GNU binutils, the printable character strings are extracted from the binary to compile. (6)Nmap 6.40 Security scanner to inspect the port on the system. (7)pjlftp Software to transfer command of PJL (language used for print job).

<Content of the Performed Penetration Testing>

Table 7-4 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 7-4 Overview of Penetration Testing

Concerned vulnerabilities	Overview of Testing
(1) Vulnerability	Testing was performed to confirm the possibility of abusing by using the tool such as Nessus and behavior inspection.
(2) Vulnerability	Testing was performed to confirm the possibility of abusing by using the tool such as Nessus and result analysis. Testing was performed to confirm that information cannot be illegally acquired and falsified, by transferring the PJL command that has concerns about illegal acquisition and falsification of information.
(3) Vulnerability	Testing was performed to confirm that the forced power ON/OFF does not affect the security functions of initialization process, screen display, and so on.
(4) Vulnerability	Testing was performed to confirm that information to affect security functions is not leaked from the data transferred between the card reader, MFP, and the external authentication servers.
(5) Vulnerability	Testing was performed to confirm that there is not the situation to be operated with different authority from the operator, in the case which the authentication with IC card is tried in the authenticated state from the operation panel as well as in the reverse case.
(6) Vulnerability	Testing was performed to confirm whether a mechanism reducing a threat operates under a specific condition.

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.4 Evaluated Configuration

(1) Operating model
It is assumed that this TOE is installed in either bizhub 554e, bizhub 454e, bizhub 364e, bizhub 284e or bizhub 224e, which is MFP provided by KONICA MINOLTA, INC.
Because of the reason shown in 7.3.2, the evaluation is considered to be conducted with all models though the evaluation was not conducted with these all models.

(2) Setting of the TOE
The evaluation was performed with the setting of "enhanced security function" activated.
This setting is as the setting shown in the ST.

7.5 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM by submitting the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance: None

- Security functional requirements: Common Criteria Part 2 Extended

- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL3 package

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.6 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to consumers.

8. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. The submitted evidential materials were sampled, the contents were examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

2. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

3. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight review, and it was sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in the certification oversight review were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report and related evaluation deliverables, the Certification Body determined that the TOE satisfies all assurance requirements for EAL3 in the CC Part 3.

8.2 Recommendations

- This TOE depends on the following functions to counter threats and to fulfill the organisational security policies. (Refer to 4.3.)
  > ASIC installed in MFP
  > IC card, IC card reader, exclusive driver
  > Active Directory
  > Difficulty of obtaining the information of setting values such as passwords which remains in SSD

  The reliability of these functions is not assured in this evaluation, and it depends on procurement personnel's judgment.

- The information to authenticate IC card with Active Directory server is registered to Active Directory at the time of issuing the IC card by a corporation which issues IC card.

- If FAX unit as an optional part is not installed, FAX unit control function that is one of the security functions is invalid. (It does not affect the operation of other security functions.)

9. Annexes

There is no annex.

10. Security Target

Security Target [12] of the TOE is provided as a separate document along with this Certification Report.

bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e PKI Card System Control Software Security Target Version 1.02 (April 10, 2014) KONICA MINOLTA, INC.

11. Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the TOE used in this report are listed below.

CAC	Common Access Card
DNS	Domain Name System
FTP	File Transfer Protocol
HDD	Hard Disk Drive
MFP	Multiple Function Peripheral
MIB	Management Information Base
NVRAM	Non-Volatile Random Access Memory
PIV	Personal ID Verification
RAM	Random Access Memory
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
SSL	Secure Socket Layer
S/MIME	Secure Multipurpose Internet Mail Extensions
USB	Universal Serial Bus

The definitions of terms used in this report are listed below.

CAC	IC card which is issued by the certification authority in the US Department of Defense.
External network	Network that access is restricted with intra-office LAN, which the TOE is connected, by firewall, etc.
FTP	File Transfer Protocol used at TCP/IP network.
Intra-office LAN	Network which the TOE is connected and is connected to the external network through firewall, etc.
MIB	Various setting information that the various devices managed using SNMP open.
NVRAM	Random access memory that has a non-volatile and memory keeping character even at the power OFF.
PIV	Personal ID verification method to carry out using a certificate issued by a federal office or using related information.
S/MIME	Standard of e-mail encryption method. Transmitting and receiving the encrypted messages using RSA public key encryption method. An electric certificate issued by certification authority is necessary.
SNMP	Protocol to manage various devices through network.
SSL	Protocol to transmit information by encrypting through the Internet.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, March 2012, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, April 2013, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, April 2013, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001 (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002 (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003 (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004 (Japanese Version 1.0, November 2012)

[12] bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e PKI Card System Control Software Security Target Version 1.02 (April 10, 2014) KONICA MINOLTA, INC.

[13] bizhub 554e / bizhub 454e / bizhub 364e / bizhub 284e / bizhub 224e PKI Card System Control Software Evaluation Technical Report, Version 2, April 18, 2014, Mizuho Information & Research Institute, Inc. Information Security Evaluation Office